

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-327748

(43)Date of publication of application : 10.12.1993

(51)Int.Cl. H04L 12/44  
G06F 13/00  
G09C 1/00  
H04L 9/06  
H04L 9/14

(21)Application number : 04-134876

(71)Applicant : FUJITSU LTD

(22)Date of filing : 27.05.1992

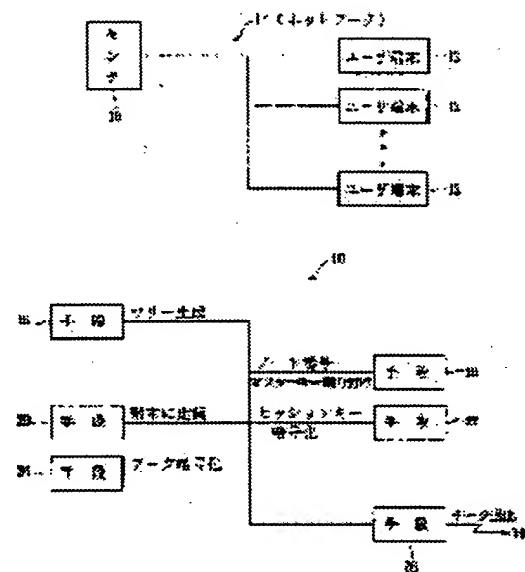
(72)Inventor : TORII NAOYA  
AKIYAMA RYOTA  
HASEBE TAKAYUKI

## (54) MULTI-ADDRESS COMMUNICATION SYSTEM

### (57)Abstract:

**PURPOSE:** To shorten the key distributing time and to decrease the number of storage keys by multi-addressing the ciphering data to a group of user terminals from a center via a star line network.

**CONSTITUTION:** A means 16 of a center 10 produces a tree which covers the center 10 through each user terminal 12. Meanwhile a means 18 of the center 10 assigns the proper numbers and the master keys to all nodes included in the tree. A means 20 defines a node proper number and a master key to each terminal 12, and a means 22 ciphers the session key with the master key of the node shown by the designated proper number. Then the means 24 ciphers the data to be multi-addressed to the terminals of the lower ranks than a node layer by means of the session key.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-327748

(43)公開日 平成5年(1993)12月10日

(51)Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 12/44				
G 0 6 F 13/00	3 5 1 Z	7368-5B		
G 0 9 C 1/00		9194-5L		
		8529-5K	H 0 4 L 11/ 00	3 4 0
		7117-5K	9/ 02	Z

審査請求 未請求 請求項の数 7 (全 30 頁) 最終頁に続く

(21)出願番号 特願平4-134876

(22)出願日 平成4年(1992)5月27日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72)発明者 鳥居 直哉

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72)発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72)発明者 長谷部 高行

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(74)代理人 弁理士 伊藤 儀一郎

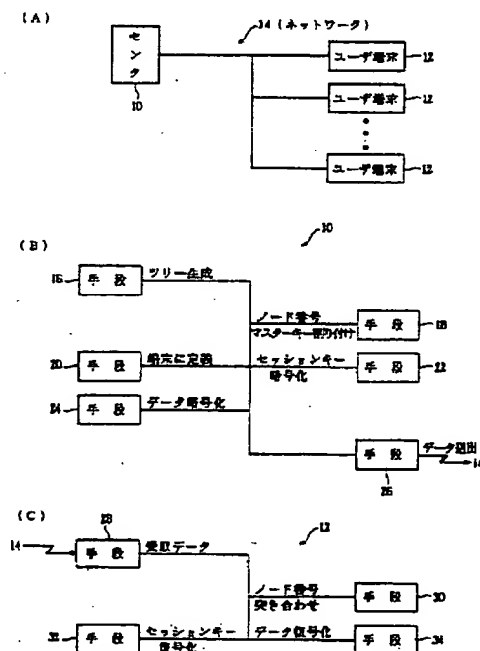
(54)【発明の名称】 同報通信システム

(57)【要約】

【目的】 本発明は、センタからユーザ端末グループへ暗号化データがスター状のネットワークを介して同報されるシステムに関し、キー配送時間の短縮、保管キーの減少が可能となる同報通信システムの提供を目的とする。

【構成】 センタ10は、各ユーザ端末12に至るツリーの生成手段16と、ツリー上に存在の全ノードへ固有番号とマスタキーを割り付ける手段18と、各ユーザ端末12にノード固有番号とマスタキーを定義する手段20と、指定の固有番号が示すノードのマスタキーでセッションキーを暗号化する手段22と、該ノードのレイヤより下位側の端末グループへ同報送信すべきデータをセッションキーで暗号化する手段24と、指定のノード固有番号と暗号化されたセッションキー及びデータとをネットワーク14へ送出する手段26と、を有する。

図1 発明及び第2発明の原理図



## 【特許請求の範囲】

【請求項 1】 単一のセンタ（１０）と多数のユーザ端末（１２）とがスター状のネットワーク（１４）で結ばれ、センタ（１０）からユーザ端末（１２）のグループへ暗号化されたデータがネットワーク（１４）を介して同報される同報通信システムにおいて、

センタ（１０）は、

センタ（１０）と全てのユーザ端末（１２）とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段（１６）と、

センタ（１０）から各ユーザ端末（１２）へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段（１８）と、各ユーザ端末（１２）についてセンタ（１０）から自端末（１２）に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段（２０）と、

指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段（２２）と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（１２）のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段（２４）と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（１４）へ送出する手段（２６）と、

を有し、

各ユーザ端末（１２）は、

センタ（１０）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（１４）を介してセンタ（１０）から受け取る手段（２８）と、

手段（２８）がネットワーク（１４）から受け取ったノード固有番号とセンタ（１０）側から予め秘密配布された自端末（１２）のノード固有番号とを突き合わせて自端末（１２）が同報送信先となる端末グループのメンバーであるか否かを判定する手段（３０）と、

自端末（１２）が同報送信先となる端末グループのメンバーであるときに手段（２８）がネットワーク（１４）から受け取ったセッションキーデータをセンタ（１０）側から予め秘密配布された自端末（１２）のマスタキーデータで復号する手段（３２）と、

手段（２８）がネットワーク（１４）から受け取ったデータを復号されたセッションキーデータで復号する手段（３４）と、

を有する、ことを特徴とした同報通信システム。

【請求項 2】 単一のセンタ（１０）と多数のユーザ端末（１２）とがスター状のネットワーク（１４）で結ばれ、センタ（１０）からユーザ端末（１２）のグループへ暗号化されたデータがネットワーク（１４）を介して

同報される同報通信システムにおいて、

センタ（１０）は、

センタ（１０）と全てのユーザ端末（１２）とが最上位のレイヤと最下位のレイヤとに各々配置されたバイナリツリーを生成する手段（１６）と、

センタ（１０）から各ユーザ端末（１２）へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段（１８）と、各ユーザ端末（１２）についてセンタ（１０）から自端末（１２）に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータを定義する手段（２０）と、

指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段（２２）と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末（１２）のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段（２４）と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク（１４）へ送出する手段（２６）と、

を有し、

各ユーザ端末（１２）は、

センタ（１０）から送出されたノード固有番号とセッションキーデータとデータとをネットワーク（１４）を介してセンタ（１０）から受け取る手段（２８）と、

手段（２８）がネットワーク（１４）から受け取ったノード固有番号とセンタ（１０）側から予め秘密配布された自端末（１２）のノード固有番号とを突き合わせて自端末（１２）が同報送信先となる端末グループのメンバーであるか否かを判定する手段（３０）と、

自端末（１２）が同報送信先となる端末グループのメンバーであるときに手段（２８）がネットワーク（１４）から受け取ったセッションキーデータをセンタ（１０）側から予め秘密配布された自端末（１２）のマスタキーデータで復号する手段（３２）と、

手段（２８）がネットワーク（１４）から受け取ったデータを復号されたセッションキーデータで復号する手段（３４）と、

を有する、

ことを特徴とした同報通信システム。

【請求項 3】 単一のセンタ（１０）と多数のユーザ端末（１２）とがスター状のネットワーク（１４）で結ばれ、センタ（１０）からユーザ端末（１２）のグループへ暗号化されたデータがネットワーク（１４）を介して同報される同報通信システムにおいて、

センタ（１０）は、

十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意す

る手段(40)と、  
センタ(10)と全てのユーザ端末(12)とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段(42)と、  
手段(40)が予め用意した最小公倍数と互いに素となる数のマスターキーデータと固有の番号とをセンタ(10)から各ユーザ端末(12)へ至るツリー中の経路上に存在した各ノードへ割り付ける手段(44)と、  
各ユーザ端末(12)についてセンタ(10)から自端末(12)へ至るツリー中の経路上に存在した全ノードの固有番号とマスターキーデータとを定義する手段(46)と、  
手段(40)が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段(40)が予め用意した最小公倍数と手段(40)が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末(12)について作成する手段(48)と、  
指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスターキーデータと手段(40)が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段(50)と、  
作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段(52)と、  
指定された固有番号が示すノードのレイヤより下位側となるユーザ端末(12)へ同報すべきデータをセッションキーデータで暗号化する手段(54)と、  
指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク(14)へ送出する手段(56)と、  
を有し、  
各ユーザ端末(12)は、  
センタ(10)から送出されたノード固有番号とセッションキーデータとデータとをネットワーク(14)を介して受け取る手段(58)と、  
手段(58)がネットワーク(14)から受け取ったノード固有番号とセンタ(10)側から予め配布された自端末(12)のノード固有番号とを突き合わせて自端末(12)が同報送信先となる端末グループのメンバーであるかを判定する手段(60)と、  
自端末(12)が同報送信先となる端末グループのメンバーであるときに自端末(12)のパスワードとセンタ(10)側から予め配布された自端末(12)のマスターキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段(62)と、  
手段(58)がネットワーク(14)から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段(64)と、  
手段(58)がネットワーク(14)から受け取ったデータを復号されたセッションキーデータで復号する手段

(66)と、

を有する、

ことを特徴とした同報通信システム。

【請求項4】 単一のセンタ(10)と多数のユーザ端末(12)とがスター状のネットワーク(14)で結ばれ、センタ(10)からユーザ端末(12)のグループへ暗号化されたデータがネットワーク(14)を介して同報される同報通信システムにおいて、

センタ(10)は、

十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段(40)と、

センタ(10)と全てのユーザ端末(12)とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段(42)と、

手段(40)が予め用意した最小公倍数と互いに素となる乱数のマスターキーデータと固有の番号とをセンタ(10)から各ユーザ端末(12)へ至るツリー中の経路上に存在した各ノードへ割り付ける手段(44)と、

各ユーザ端末(12)についてセンタ(10)から自端末(12)へ至るツリー中の経路上に存在した全ノードのマスターキーデータと固有番号とを定義する手段(46)と、

手段(40)が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段(40)が予め用意した最小公倍数と手段(40)が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末(12)について作成する手段(48)と、  
指定された固有番号に対応したレイヤよりセンタ(10)側に配置された各ノードのマスターキーデータと手段(40)が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段(50)と、  
作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段(52)と、  
指定された固有番号が示すノードのレイヤより下位側となるユーザ端末(12)へ同報すべきデータをセッションキーデータで暗号化する手段(54)と、  
指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク(14)へ送出する手段(56)と、

を有し、  
各ユーザ端末(12)は、  
センタ(10)から送出されたノード固有番号とセッションキーデータとデータとをネットワーク(14)から受け取る手段(58)と、  
手段(58)がネットワーク(14)から受け取ったノード固有番号とセンタ(10)側から予め配布された自端末(12)のノード固有番号とを突き合わせて自端末(12)が同報送信先となる端末グループのメンバーであ

る、

各ユーザ端末(12)は、

センタ(10)から送出されたノード固有番号とセッションキーデータとデータとをネットワーク(14)から受け取る手段(58)と、

手段(58)がネットワーク(14)から受け取ったノード固有番号とセンタ(10)側から予め配布された自端末(12)のノード固有番号とを突き合わせて自端末(12)が同報送信先となる端末グループのメンバーであ

るか否かを判定する手段(60)と、  
自端末(12)が同報送信先となる端末グループのメンバーであるときに自端末(12)のパスワードとセンタ(10)側から予め配布された自端末(12)のマスターキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段(62)と、  
手段(58)がネットワーク(14)から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段(64)と、  
手段(58)がネットワーク(14)から受け取ったデータを復号されたセッションキーデータで復号する手段(66)と、  
を有する、  
ことを特徴とした同報通信システム。

【請求項5】 単一のセンタ(10)と多数のユーザ端末(12)とがスター状のネットワーク(14)で結ばれ、センタ(10)からユーザ端末(12)のグループへ暗号化されたデータがネットワーク(14)を介して同報される同報通信システムにおいて、

センタ(10)は、  
十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段(70)と、

センタ(10)と全てのユーザ端末(12)とが最上位のレイヤと最下位のレイヤとに各々配置され最上位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段(72)と、

手段(70)が予め用意した最小公倍数と互いに素となる乱数のマスターキーデータと固有の番号とをセンタ(10)から各ユーザ端末(12)へ至るツリー中の経路上に存在した各ノードへ割り付ける手段(74)と、

各ユーザ端末(12)についてセンタ(10)から自端末(12)へ至るツリー中の経路上に存在した全ノードの固有番号とマスターキーデータとを定義する手段(76)と、

上位側のノードが同一でデータを同報すべきグループのメンバーとなるユーザ端末(12)についてグループキーデータを定義する手段(78)と、

手段(70)が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段(70)が予め用意した最小公倍数と手段(70)が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末(12)について作成する手段(80)と、

指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスターキーデータと手段(70)が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段(82)と、

作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段(84)と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末(12)へ同報すべきデータをセッションキーデータで暗号化する手段(86)と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク(14)へ送出する手段(88)と、

を有し、

各ユーザ端末(12)は、

センタ(10)から送出されたノード固有番号とセッションキーデータとデータとをネットワーク(14)を介して受け取る手段(90)と、

手段(90)がネットワーク(14)から受け取ったノード固有番号とセンタ(10)側から予め配布された自端末(12)のノード固有番号とを突き合わせて自端末(12)が同報送信先となる端末グループのメンバーであるか否かを判定する手段(92)と、

自端末(12)が同報送信先となる端末グループのメンバーであるときに自端末(12)のパスワードとセンタ(10)側から予め配布された自端末(12)のマスターキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段(94)と、

手段(90)がネットワーク(14)から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段(96)と、

手段(90)がネットワーク(14)から受け取ったデータを復号されたセッションキーデータで復号する手段(98)と、

を有する、

ことを特徴とした同報通信システム。

【請求項6】 単一のセンタ(10)と多数のユーザ端末(12)とがスター状のネットワーク(14)で結ばれ、センタ(10)からユーザ端末(12)のグループへ暗号化されたデータがネットワーク(14)を介して同報される同報通信システムにおいて、

センタ(10)は、

十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段(70)と、

センタ(10)と全てのユーザ端末(12)とが最上位のレイヤと最下位のレイヤとに各々配置され最上位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたバイナリツリーを生成する手段(72)と、

手段(70)が予め用意した最小公倍数と互いに素となる乱数のマスターキーデータと固有の番号とをセンタ(10)から各ユーザ端末(12)へ至るツリー中の経路上に存在した各ノードへ割り付ける手段(74)と、

各ユーザ端末(12)についてセンタ(10)から自端末(12)へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段(76)と、

上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末(12)についてグループキーデータを定義する手段(78)と、

手段(70)が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段(70)が予め用意した最小公倍数と手段(70)が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末(12)について作成する手段(80)と、

指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段(70)が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段(82)と、

作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段(84)と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末(12)へ同報すべきデータをセッションキーデータで暗号化する手段(86)と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク(14)へ送出する手段(88)と、

を有し、

各ユーザ端末(12)は、

センタ(10)から送出されたノード固有番号とセッションキーデータとデータとをネットワーク(14)を介して受け取る手段(90)と、

手段(90)がネットワーク(14)から受け取ったノード固有番号とセンタ(10)側から予め配布された自端末(12)のノード固有番号とを突き合わせて自端末(12)が同報送信先となる端末グループのメンバであるか否かを判定する手段(92)と、

自端末(12)が同報送信先となる端末グループのメンバであるときに自端末(12)のパスワードとセンタ

(10)側から予め配布された自端末(12)のマスタキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段(94)と、

手段(90)がネットワーク(14)から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段(96)と、

手段(90)がネットワーク(14)から受け取ったデータを復号されたセッションキーデータで復号する手段(98)と、

を有する、

ことを特徴とした同報通信システム。

【請求項7】 単一のセンタ(10)と多数のユーザ端末(12)とがスター状のネットワーク(14)で結ばれ、センタ(10)からユーザ端末(12)のグループへ暗号化されたデータがネットワーク(14)を介して同報される同報通信システムにおいて、

センタ(10)は、

十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段(70)と、

センタ(10)と全てのユーザ端末(12)とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段(72)と、

手段(70)が予め用意した最小公倍数と互いに素となる数のマスタキーデータと固有の番号とをセンタ(10)から各ユーザ端末(12)へ至るツリー中の経路上に存在した各ノードへ割り付ける手段(74)と、

各ユーザ端末(12)についてセンタ(10)から自端末(12)へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段(76)と、

上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末(12)についてグループキーデータを定義する手段(78)と、

手段(70)が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段(70)が予め用意した最小公倍数と手段(70)が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末(12)について作成する手段(80)と、

指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段(70)が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段(82)と、

作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段(84)と、

指定された固有番号が示すノードのレイヤより下位側となるユーザ端末(12)へ同報すべきデータをセッションキーデータで暗号化する手段(86)と、

指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク(14)へ送出する手段(88)と、

を有し、

各ユーザ端末(12)は、

センタ(10)から送出されたノード固有番号とセッションキーデータとデータとをネットワーク(14)を介して受け取る手段(90)と、

手段(90)がネットワーク(14)から受け取ったノ

ード固有番号とセンタ(10)側から予め配布された自端末(12)のノード固有番号とを突き合わせて自端末(12)が同報送信先となる端末グループのメンバであるか否かを判定する手段(92)と、  
自端末(12)が同報送信先となる端末グループのメンバであるときに自端末(12)のパスワードとセンタ(10)側から予め配布された自端末(12)のマスターキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段(94)と、  
手段(90)がネットワーク(14)から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段(96)と、  
手段(90)がネットワーク(14)から受け取ったデータを復号されたセッションキーデータで復号する手段(98)と、  
を有する、  
ことを特徴とした同報通信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、単一のセンタからユーザ端末のグループへ暗号化されたデータがスター状のネットワークを介して同報される同報通信システムに関する。

【0002】衛星を介してデータを送信する場合で、契約などにより限られたユーザの端末だけにそのデータをセンタから同報するときには、他の端末で同報のデータを傍受されないように、このデータが暗号化される。

【0003】

【従来の技術】センタにホストコンピュータが有線回線を介して接続され、各ユーザ端末の要求に応じ、センタとユーザの端末との間で衛星回線を介してデータの送受信が行なわれる。

【0004】そのデータ通信はセンタで一元的に管理され、多くの場合、データ通信に際し、個々のユーザ回線を多重化して送受信を行なう個別送信モードと複数のユーザをメンバとするグループにセンタより暗号化されたデータを同報する同報モードとのいずれかが選択される。

【0005】ここで同報モードが選択されると、グループ暗号通信のためのセッションキーがセンタで生成され、また、ユーザ端末毎にセッションキー配送用のマスターキーが定められる。そして、セッションキーはマスターキーで暗号化されて各ユーザ端末へ配送され(暗号化セッションキー)、暗号化された同報データの復元に各ユーザ端末で利用される。

【0006】

【発明が解決しようとする課題】同報先となる端末グループを構成するユーザ端末の全てに、該当の暗号化セッションキーを配送する場合、グループメンバ(ユーザ端

末)の数とともにキー配送の所要時間が増加する。

【0007】そのユーザ端末の総数は一般に数百万に達し、同報先となる端末グループのメンバ数も極めて多いものとなる。したがって、セッションキーの配送に長時間を要する。

【0008】また、全てのマスターキーを予め配布して各ユーザ端末で管理する方式の場合には、センタ局側で管理すべきグループキーがユーザ端末側のものを含めて $2^{a \cdot b} \cdot (t-1)$ ( $t$ はユーザ端末数を意味し、 $a \cdot b$ は $a$ の $b$ 乗を意味する)本となり、ユーザ端末側においても $2^{a \cdot b} \cdot (t-1)$ 本のマスターキーを保管することが必要となるので、ユーザ端末数が数百万となることから、キー保管のデータ量が膨大なものとなる。

【0009】本発明は上記従来の事情に鑑みてなされたものであり、その目的は、キー配送時間の短縮、保管キーの減少が可能となる同報通信システムを提供することにある。

【0010】

【課題を解決するための手段】

／\* 第1発明 \*/

図1(A)において、単一のセンタ10と多数のユーザ端末12とがスター状のネットワーク14で結ばれ、センタ10からユーザ端末12のグループへ暗号化されたデータがネットワーク14を介して同報される。

【0011】この図1(A)のセンタ10は、同図(B)において、センタ10と全てのユーザ端末12とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段16と、センタ10から各ユーザ端末12へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスターキーデータとを割り付ける手段18と、各ユーザ端末12についてセンタ10から自端末12に至るツリー中の経路上に存在した全ノードの固有番号とマスターキーデータを定義する手段20と、指定された固有番号が示すノードのマスターキーデータで乱数のセッションキーデータを暗号化する手段22と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段24と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク14へ送出する手段26と、を有する。

【0012】また図1(A)の各ユーザ端末12は、同図(C)において、センタ10から送出されたノード固有番号とセッションキーデータとデータとをネットワーク14を介してセンタ10から受け取る手段28と、手段28がネットワーク14から受け取ったノード固有番号とセンタ10側から予め秘密配布された自端末12のノード固有番号とを突き合わせて自端末12が同報送信先となる端末グループのメンバであるか否かを判定する手段30と、自端末12が同報送信先となる端末グルー



ブのメンバであるときに手段 28 がネットワーク 14 から受け取ったセッションキーデータをセンタ 10 側から予め秘密配布された自端末 12 のマスタキーデータで復号する手段 32 と、手段 28 がネットワーク 14 から受け取ったデータを復号されたセッションキーデータで復号する手段 34 と、を有する。

【0013】／＊ 第 2 発明 ＊／

図 1 (A) において、単一のセンタ 10 と多数のユーザ端末 12 とがスター状のネットワーク 14 で結ばれ、センタ 10 からユーザ端末 12 のグループへ暗号化されたデータがネットワーク 14 を介して同報される。

【0014】この図 1 (A) のセンタ 10 は、同図

(B) において、センタ 10 と全てのユーザ端末 12 とが最上位のレイヤと最下位のレイヤとに各々配置されたバイナリツリーを生成する手段 16 と、センタ 10 から各ユーザ端末 12 へ至るツリー中の経路上に存在した全てのノードへ固有の番号と乱数のマスタキーデータとを割り付ける手段 18 と、各ユーザ端末 12 についてセンタ 10 から自端末 12 に至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータを定義する手段 20 と、指定された固有番号が示すノードのマスタキーデータで乱数のセッションキーデータを暗号化する手段 22 と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末 12 のグループへ同報送信すべきデータをセッションキーデータで暗号化する手段 24 と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク 14 へ送出する手段 26 と、を有する。

【0015】また図 1 (A) の各ユーザ端末 12 は、同図 (C) において、センタ 10 から送出されたノード固有番号とセッションキーデータとデータとをネットワーク 14 を介してセンタ 10 から受け取る手段 28 と、手段 28 がネットワーク 14 から受け取ったノード固有番号とセンタ 10 側から予め秘密配布された自端末 12 のノード固有番号とを突き合わせて自端末 12 が同報送信先となる端末グループのメンバであるか否かを判定する手段 30 と、自端末 12 が同報送信先となる端末グループのメンバであるときに手段 28 がネットワーク 14 から受け取ったセッションキーデータをセンタ 10 側から予め秘密配布された自端末 12 のマスタキーデータで復号する手段 32 と、手段 28 がネットワーク 14 から受け取ったデータを復号されたセッションキーデータで復号する手段 34 と、を有する。

【0016】／＊ 第 3 発明 ＊／

図 2 (A) において、単一のセンタ 10 と多数のユーザ端末 12 とがスター状のネットワーク 14 で結ばれ、センタ 10 からユーザ端末 12 のグループへ暗号化されたデータがネットワーク 14 を介して同報される。

【0017】この図 2 (A) のセンタ 10 は、同図

(B) において、十分に大きな一対の素数と両素数の乗

算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段 40 と、センタ 10 と全てのユーザ端末 12 とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段 42 と、手段 40 が予め用意した最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とをセンタ 10 から各ユーザ端末 12 へ至るツリー中の経路上に存在した各ノードへ割り付ける手段 44 と、各ユーザ端末 12 についてセンタ 10 から自端末 12 へ至るツリー中の経路上に存在した全ノードの固有番号とマスタキーデータとを定義する手段 46 と、手段 40 が予め用意した最小公倍数と互いに素となるパスワードと該当のマスタキーデータと手段 40 が予め用意した最小公倍数と手段 40 が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末 12 について作成する手段 48 と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段 40 が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段 50 と、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段 52 と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末 12 へ同報すべきデータをセッションキーデータで暗号化する手段 54 と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク 14 へ送出する手段 56 と、を有する。

【0018】また図 2 (A) の各ユーザ端末 12 は、同図 (C) において、センタ 10 が送出したノード固有番号とセッションキーデータとデータとをネットワーク 14 から受け取る手段 58 と、手段 58 がネットワーク 14 から受け取ったノード固有番号とセンタ 10 側から予め配布された自端末 12 のノード固有番号とを突き合わせて自端末 12 が同報送信先となる端末グループのメンバであるか否かを判定する手段 60 と、自端末 12 が同報送信先となる端末グループのメンバであるときに自端末 12 のパスワードとセンタ 10 側から予め配布された自端末 12 のマスタキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段 62 と、手段 58 がネットワーク 14 から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段 64 と、手段 58 がネットワーク 14 から受け取ったデータを復号されたセッションキーデータで復号する手段 66 と、を有する。

【0019】／＊ 第 4 発明 ＊／

図 2 (A) において、単一のセンタ 10 と多数のユーザ端末 12 とがスター状のネットワーク 14 で結ばれ、センタ 10 からユーザ端末 12 のグループへ暗号化されたデータがネットワーク 14 を介して同報される。

【0020】この図 2 (A) のセンタ 10 は、同図

(B)において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段40と、センタ10と全てのユーザ端末12とが最上位のレイヤと最下位のレイヤとに各々配置されたツリーを生成する手段42と、手段40が予め用意した最小公倍数と互いに素となる数のマスターキーデータと固有の番号とをセンタ10から各ユーザ端末12へ至るツリー中の経路上に存在した各ノードへ割り付ける手段44と、各ユーザ端末12についてセンタ10から自端末12へ至るツリー中の経路上に存在した全ノードのマスターキーデータと固有番号とを定義する手段46と、手段40が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段40が予め用意した最小公倍数と手段40が予め用意した乗算結果とにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末12について作成する手段48と、指定された固有番号に対応したノード及び該ノード下位側のレイヤに配置された各ノードのマスターキーデータと手段40が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段50と、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段52と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12へ同報すべきデータをセッションキーデータで暗号化する手段54と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク14へ送出する手段56と、を有する。

【0021】また図2(A)の各ユーザ端末12は、同図(C)において、センタ10が送出したノード固有番号とセッションキーデータとデータとをネットワーク14から受け取る手段58と、手段58がネットワーク14から受け取ったノード固有番号とセンタ10側から予め配布された自端末12のノード固有番号とを突き合わせて自端末12が同報送信先となる端末グループのメンバーであるか否かを判定する手段60と、自端末12が同報送信先となる端末グループのメンバーであるときに自端末12のパスワードとセンタ10側から予め配布された自端末12のマスターキーデータ及びキー生成データとを用いてキー暗号化キーデータを作成する手段62と、手段58がネットワーク14から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段64と、手段58がネットワーク14から受け取ったデータを復号されたセッションキーデータで復号する手段66と、を有する。

【0022】／＊ 第5発明 ＊／

図3(A)において、単一のセンタ10と多数のユーザ端末12とがスター状のネットワーク14で結ばれ、センタ10からユーザ端末12のグループへ暗号化されたデータがネットワーク14を介して同報される。

【0023】この図3(A)のセンタ10は、同図

(B)において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段70と、センタ10と全てのユーザ端末12とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段72と、手段70が予め用意した最小公倍数と互いに素となる乱数のマスターキーデータと固有の番号とをセンタ10から各ユーザ端末12へ至るツリー中の経路上に存在した各ノードへ割り付ける手段74と、各ユーザ端末12についてセンタ10から自端末12へ至るツリー中の経路上に存在した全ノードの固有番号とマスターキーデータとを定義する手段76と、上位側のノードが同一でデータを同報すべきグループのメンバーとなるユーザ端末12についてグループキーデータを定義する手段78と、手段70が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段70が予め用意した最小公倍数と手段70が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末12について作成する手段80と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスターキーデータと手段70が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段82と、を有する。

【0024】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段84と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12へ同報すべきデータをセッションキーデータで暗号化する手段86と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク14へ送出する手段88と、を有する。

【0025】また図3(A)の各ユーザ端末12は、同図(C)において、センタ10が送出したノード固有番号とセッションキーデータとデータとをネットワーク14から受け取る手段90と、手段90がネットワーク14から受け取ったノード固有番号とセンタ10側から予め配布された自端末12のノード固有番号とを突き合わせて自端末12が同報送信先となる端末グループのメンバーであるか否かを判定する手段92と、自端末12が同報送信先となる端末グループのメンバーであるときに自端末12のパスワードとセンタ10側から予め配布された自端末12のマスターキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段94と、手段90がネットワーク14から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段96と、手段90がネットワ

ーク 14 から受け取ったデータを復号されたセッションキーデータで復号する手段 98 と、を有する。

【0026】／＊ 第 6 発明 ＊／

図 3 (A) において、単一のセンタ 10 と多数のユーザ端末 12 とがスター状のネットワーク 14 で結ばれ、センタ 10 からユーザ端末 12 のグループへ暗号化されたデータがネットワーク 14 を介して同報される。

【0027】この図 3 (A) のセンタ 10 は、同図

(B) において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段 70 と、センタ 10 と全てのユーザ端末 12 とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたバイナリツリーを生成する手段 72 と、手段 70 が予め用意した最小公倍数と互いに素となる乱数のマスターキーデータと固有の番号とをセンタ 10 から各ユーザ端末 12 へ至るツリー中の経路上に存在した各ノードへ割り付ける手段 74 と、各ユーザ端末 12 についてセンタ 10 から自端末 12 へ至るツリー中の経路上に存在した全ノードのマスターキーデータと固有番号とを定義する手段 76 と、上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末 12 についてグループキーデータを定義する手段 78 と、手段 70 が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段 70 が予め用意した最小公倍数と手段 70 が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末 12 について作成する手段 80 と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスターキーデータと手段 70 が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段 82 と、を有する。

【0028】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段 84 と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末 12 へ同報すべきデータをセッションキーデータで暗号化する手段 86 と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク 14 へ送出する手段 88 と、を有する。

【0029】また図 3 (A) の各ユーザ端末 12 は、同図 (C) において、センタ 10 が送出したノード固有番号とセッションキーデータとデータとをネットワーク 14 から受け取る手段 90 と、手段 90 がネットワーク 14 から受け取ったノード固有番号とセンタ 10 側から予め配布された自端末 12 のノード固有番号とを突き合わせて自端末 12 が同報送信先となる端末グループのメンバであるか否かを判定する手段 92 と、自端末 12 が同

報送信先となる端末グループのメンバであるときに自端末 12 のパスワードとセンタ 10 側から予め配布された自端末 12 のマスターキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段 94 と、手段 90 がネットワーク 14 から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段 96 と、手段 90 がネットワーク 14 から受け取ったデータを復号されたセッションキーデータで復号する手段 98 と、を有する。

【0030】／＊ 第 7 発明 ＊／

図 3 (A) において、単一のセンタ 10 と多数のユーザ端末 12 とがスター状のネットワーク 14 で結ばれ、センタ 10 からユーザ端末 12 のグループへ暗号化されたデータがネットワーク 14 を介して同報される。

【0031】この図 3 (A) のセンタ 10 は、同図

(B) において、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の最小公倍数とを予め用意する手段 70 と、センタ 10 と全てのユーザ端末 12 とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーを生成する手段 72 と、手段 70 が予め用意した最小公倍数と互いに素となる数のマスターキーデータと固有の番号とをセンタ 10 から各ユーザ端末 12 へ至るツリー中の経路上に存在した各ノードへ割り付ける手段 74 と、各ユーザ端末 12 についてセンタ 10 から自端末 12 へ至るツリー中の経路上に存在した全ノードの固有番号とマスターキーデータとを定義する手段 76 と、上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末 12 についてグループキーデータを定義する手段 78 と、手段 70 が予め用意した最小公倍数と互いに素となるパスワードと該当のマスターキーデータと手段 70 が予め用意した最小公倍数と手段 70 が予め用意した乗算結果とグループキーデータとにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末 12 について作成する手段 80 と、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスターキーデータと手段 70 が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する手段 82 と、を有する。

【0032】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータを暗号化する手段 84 と、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末 12 へ同報すべきデータをセッションキーデータで暗号化する手段 86 と、指定されたノード固有番号と暗号化されたセッションキーデータと暗号化されたデータとをネットワーク 14 へ送出する手段 88 と、を有する。

【0033】また図 3 (A) の各ユーザ端末 12 は、同

図(C)において、センタ10が送出したノード固有番号とセッションキーデータとデータとをネットワーク14から受け取る手段90と、手段90がネットワーク14から受け取ったノード固有番号とセンタ10側から予め配布された自端末12のノード固有番号とを突き合わせて自端末12が同報送信先となる端末グループのメンバーであるか否かを判定する手段92と、自端末12が同報送信先となる端末グループのメンバーであるときに自端末12のパスワードとセンタ10側から予め配布された自端末12のマスタキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータを作成する手段94と、手段90がネットワーク14から受け取ったセッションキーデータを生成されたキー暗号化キーデータで復号する手段96と、手段90がネットワーク14から受け取ったデータを復号されたセッションキーデータで復号する手段98と、を有する。

【0034】

【作用】

／＊ 第1発明 第2発明 ＊／

ユーザ端末12の総数が与えられることにより、グループキー配送用のツリーが作成される。

【0035】このツリーはセンタ10が配置されたルートの最上位レイヤから2枝またはそれ以上に分岐しながら伸長し、レイヤ(i)は枝分岐毎に0, 1, 2, ...と下位側へ増加し、各レイヤにおけるノード(j)の数はその上位側レイヤからの分岐倍となり、ツリーは最下位レイヤのノード数がユーザ端末12の総数に達したときに伸長を停止する。

【0036】図4においてはユーザ端末12の総数が8とされたバイナリツリーが示されており、レイヤが0から3まで増加してユーザ端末12の総数に対応したノード数が7へ達したときに、ツリーがその伸長を停止する。

【0037】さらに、センタ10から各ユーザ端末12へ至るツリー中の経路上に存在した全てのノードに、固有の番号NijとマスタキーデータKijとが割り付けられる。

【0038】図4においては、固有番号N00, N10, N11, N20, N21, N22, N23, N30, N31, N32, N33, N34, N35, N36, N37とマスタキーデータK00, K10, K11, K20, K21, K22, K23, K30, K31, K32, K33, K34, K35, K36, K37とが各ノードに割り当てられる。

【0039】そして、センタ10からユーザ端末12へ至るツリー経路上に存在したノードの固有番号NijとマスタキーデータKijが調べられ、ノード固有番号NijとマスタキーデータKij(の並び)で示される各経路が該当のユーザ端末12に定義される。

【0040】図4においては、最下位のレイヤ3に配置

されている第4ノードのユーザ端末12にノード番号N33, N21, N10, N00とマスタキーデータK33, K21, K10およびK00が定義される。

【0041】ただし、マスタキーデータKijは乱数を発生させることにより得られており、ノード固有番号Nij, マスタキーデータKijは該当のユーザ端末12へ秘密裏に配布される。

【0042】ここで、ユーザ端末12が配置された最下位のレイヤより上位側のレイヤに属するノード番号Nijの指定で、枝分岐数のユーザ端末12を指定できる。例えば図4においてノードN21を指定することでノード番号N32, N33を指定できる。

【0043】したがって、センタ10の最上位レイヤに近いレイヤのノード番号Nijを指定することにより、そのノードから分岐した経路の先端に配置されているユーザ端末12の全てを一括してグループ指定することが可能となる。

【0044】複数のユーザ端末12をメンバーとするグループへセンタ10より暗号化されたデータを同報するグループ送信に際しては、グループメンバーのユーザ端末12をより多くグループ化できるように、ツリー上位側となるノードの位置と数が算出されてそれらノードの固有番号が指定され、指定された固有番号が示すノードのマスタキーデータでセッションキーのデータが暗号化される。

【0045】このセッションキーのデータも乱数を発生させることにより得られており、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12のグループへ同報送信すべきデータはセッションキーデータで暗号化され、指定されたノード固有番号とともにセンタ10からネットワーク14へ送出される。

【0046】また各ユーザ端末12では、ネットワーク14から受け取ったノード固有番号とセンタ10側から予め秘密配布された自端末12のノード固有番号との突き合わせで、自端末12が同報送信先となる端末グループのメンバーであるか否かが判定される。

【0047】このときに自端末12が同報送信先となる端末グループのメンバーであることが確認されると、ネットワーク14から受け取ったセッションキーデータがセンタ10側から予め秘密配布された自端末12のマスタキーデータで復号され、同ネットワーク14から受け取った同報送信データが復号後のセッションキーデータを用いて復号される。

【0048】／＊ 第3発明 第4発明 ＊／

これらの発明においてもツリー構造を用いたキー配布が行なわれる。ただし、特開平2-301240などで示される方式が適用される。

【0049】センタ10において、十分に大きな一対の素数p, q(SRA暗号システムの意味で大きな良い素数とすることが好ましい)と両素数の乗算結果 $n = p \times$

qと両素数から各々定められた一対の数(p-1, q-1)の最小公倍数Lとが予め用意される。

【0050】そしてツリーが生成されると、第3発明では最小公倍数Lと互いに素となる乱数のマスタキーデータ(乱数を発生させて最小公倍数Lと互いに素となるか否かを調べ、素の場合にはこれを採用し、素でない場合にはまた乱数を発生させて最小公倍数Lと互いに素となるか否かを調べる)と固有の番号とが、センタ10から各ユーザ端末12へ至るツリー中の経路上に存在した各ノードへ、割り付けられる。

【0051】第4発明では、素数発生回路などの利用により、最小公倍数Lと互いに素となる数が直接生成され、乱数が最小公倍数Lと互いに素であるかどうかを調べる処理が省略される。

【0052】各ユーザ端末12についてマスタキーデータと固有番号とが定義されると、最小公倍数Lと互いに素となるパスワード、該当のマスタキーデータ、最小公倍数L、乗算結果nにより定まるキー生成データを、指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末12について作成する処理が行なわれる。

【0053】例えば、全てのノードについて  $K_{ij} * (1/K_{ij}) = 1 \pmod{L}$  となる  $1/K_{ij}$  を計算し、ユーザ端末12のパスワードPWs (s=0, 1, ..., t-1) を入力し、パスワードPWsが最小公倍数Lと互いに素か否かを検査し、素の場合にはそのパスワードを用いてキー生成データを作成し、素でない場合にはパスワードPWsを再度入力する処理が行なわれる。

【0054】各ユーザ端末12のキー生成データZs (s=0, 1, ..., t-1) は図5のようにして算出でき(公開鍵: マスタキー)、該当のキー生成データZs (s=0, 1, ..., t-1)、ノード固有番号Nij及びそのツリー公開鍵のマスタキーデータKijはセンタ10から各ユーザ端末12へ配布される。

【0055】図6(A)ではユーザ端末12の数が8の場合におけるツリーとキー生成データが対応して示されており、ノード固有番号N32のユーザ端末12にはノード固有番号(N32, N21, N10, N00)、マ

$$KG_{kj} = Z_j * (PW_j * K_{k-1j} * K_{k-2j} * \dots * K_{rj}) \pmod{n} \\ = C * (1 / (K_{0j} * \dots * K_{kj})) \pmod{n}$$

のように、パスワードをキー生成データZijにべき乗してから下位側レイヤにおけるノードのキーデータKij (i=k+1, ..., r) を巾乗することで、キー暗号化キーデータKGkjを作成できる。図6(A)の場合、ノード固有番号32のユーザ端末12は同図(B)のキー暗号化キーデータ(マスタキー)を作成できる。

【0063】キー暗号化キーデータが作成されると、ネ

スタキーデータ(K32, K21, K10, K00)、キー生成データ(Z32)が配布される。

【0056】グループ送信の開始時にノード固有番号が指定されると、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと乗算結果nとにより定まるキー暗号化キーデータが作成される。

【0057】例えばノード固有番号Nkjの場合、 $KG_{kj} = C * (1 / (K_{0j} * K_{1j} * \dots * K_{kj})) \pmod{n}$  のように、キーデータKij (i=0, 1, ..., k) と対応のキーデータ  $1/K_{ij}$  (i=0, 1, ..., k) を値C(図5参照)に巾乗することで、キー暗号化キーデータKGkjを作成できる。

【0058】キー暗号化キーデータが作成されると、乱数を発生させることによってセッションキーデータが生成され、このセッションキーデータがキー暗号化キーデータで暗号化される。

【0059】さらに、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12へ同報すべきデータをセッションキーデータで暗号化され、指定されたノード固有番号、暗号化されたセッションキーデータ、暗号化されたデータがネットワーク14へ送出される。

【0060】各ユーザ端末12においては、ネットワーク14から受け取ったノード固有番号とセンタ10側から予め配布された自端末12のノード固有番号とが突き合わせられ、自端末12が同報送信先となる端末グループのメンバであるか否かが判定される。

【0061】そして、自端末12が同報送信先となる端末グループのメンバであることが確認されると、自端末12のパスワード(パスワードは各ユーザが所持する)、センタ10側から予め配布された自端末12のマスタキーデータ及びキー生成データ(多くの場合、キー生成データは磁気カードやICカードに書き込まれる)を用いてキー暗号化キーデータが作成される。

【0062】例えばノード固有番号Nkjのユーザ端末の場合、

$$KG_{kj} = Z_j * (PW_j * K_{k-1j} * K_{k-2j} * \dots * K_{rj}) \pmod{n}$$

ネットワーク14から受け取ったセッションキーデータがこのキー暗号化キーデータを用いて復号され、ネットワーク14から受け取った同報送信データが復号後のセッションキーデータで復号される。

【0064】／\* 第5発明 第6発明 第7発明 \*

これらの発明においても、十分に大きな一対の素数と両素数の乗算結果と両素数から各々定められた一対の数の

最小公倍数とが予め用意される。ただし、センタ10と全てのユーザ端末12とが最上位のレイヤと最下位のレイヤとに各々配置され最下位の上位側となるレイヤのノード数がより上位側となるレイヤのノード数を越えて設定されたツリーが生成される。

【0065】例えば、最下位レイヤの上位側となるレイヤのノード数がより上位側となるレイヤの2倍に設定された場合で、ユーザ端末12の数が8とされたときには、図7に示されるツリーが生成される。

【0066】そして、最小公倍数と互いに素となる乱数のマスタキーデータと固有の番号とがセンタ10から各ユーザ端末12へ至るツリー中の経路上に存在した各ノードへ割り付けられ、各ユーザ端末12についてセンタ10から自端末12へ至るツリー中の経路上に存在した全ノードのマスタキーデータと固有番号とが定義されると、上位側のノードが同一でデータを同報すべきグループのメンバとなるユーザ端末12についてグループキーデータ $KK_{ij}$  ( $i$ : 最下位レイヤの上位側となるレイヤにおけるノードの通し番号,  $j$ : グループ内の通し番号) が定義される。

【0067】図8では最下位レイヤにおけるユーザ端末12の数が8とされた場合のユーザグループ化作用が説明されており、同図(A)では2ユーザがグループ化され、同図(B)では3ユーザがグループ化される。

【0068】以上の定義が行なわれると、最小公倍数と互いに素となるパスワード、該当のマスタキーデータ、最小公倍数、乗算結果、グループキーデータにより定まるキー生成データを指定された固有番号が示すノードのレイヤより下位側となる全てのユーザ端末12について作成する処理、指定された固有番号に対応するノード及び該ノードより下位側のレイヤに配置された各ノードのマスタキーデータと手段70が予め用意した乗算結果とにより定まるキー暗号化キーデータを作成する処理が行なわれる。

【0069】例えば、 $K_{ij} * (1/K_{ij}) = 1 \bmod L$  及び  $KK_{ij} * (1/KK_{ij}) = 1 \bmod L$  となるデータ $K_{ij}$ ,  $KK_{ij}$ を計算してから、各ユーザのパスワード $PW_s$  ( $s=0, 1, \dots, t-1$ ) を入力して最小公倍数 $L$ と互いに素となるか否かを検査し、素の場合はそのパスワードを用いてキー生成データ $Z_s$ を図9のようにして作成し、素とならない場合は、パスワードを再び入力する処理が行なわれる。

【0070】各ユーザ端末12にはノード番号、マスタキーデータ、グループキーデータ及びキー生成データが配布され、例えば、図7(A)におけるノード固有番号22のユーザ端末12にはノード固有番号( $N00, N10, N22, N20, N21, N23$ ), キーデータ( $K00, K10, K22$ ), ( $KK02, KK03, KK04, KK06, KK07, KK08$ ), キー生成

データ( $Z32$ )が配布される。

【0071】さらに、作成されたキー暗号化キーデータで乱数のセッションキーデータが暗号化され、指定された固有番号が示すノードのレイヤより下位側となるユーザ端末12へ同報すべきデータがセッションキーデータで暗号化されると、指定されたノード固有番号、暗号化されたセッションキーデータ、暗号化されたデータがネットワーク14へ送出される。

【0072】また各ユーザ端末12では、ネットワーク14から受け取ったノード固有番号とセンタ10側から予め配布された自端末12のノード固有番号とを突き合わせるにより自端末12が同報送信先となる端末グループのメンバであるか否かが判定され、グループメンバであることが確認されると、自端末12のパスワードとセンタ10側から予め配布された自端末12のマスタキーデータ、キー生成データ及びグループキーデータとを用いてキー暗号化キーデータが作成される。

【0073】例えば、受信したノード固有番号が最下位レイヤでない場合、あるいは、受信したノード固有番号が最下位レイヤであるものの、受信したノード固有番号が示す最下位レイヤのユーザ端末12がグループ化されていない場合には、図10(A)で示される内容の演算が行なわれてキー暗号化キーデータ $KG_{kj}$ が作成される。

【0074】これに対し、最下位レイヤのユーザ端末12がグループ化されており、そのグループに自端末12が含まれている場合には、図10(B)で示される内容の演算が行なわれ、キー暗号化キーデータ $KG_{kj}$ が作成される(そのグループに割り当てられたグループキーデータを $KK_{jc}$ で示す)。図6のノード識別番号 $N22$ で示されるユーザ端末12は、図10(C)のようにしてキー暗号化キーデータを作成できる。

【0075】そして、ネットワーク14から受け取ったセッションキーデータが生成されたキー暗号化キーデータで復号されると、同ネットワーク14から受け取ったデータが復号される。

【0076】なお、ツリーの各レイヤにおける分岐数を3以上に設定できる。また、素数発生回路を設け、乱数が最小公倍数 $L$ と互いに素であるか否かを調べる処理を省略することも可能である。

【0077】

【実施例】図11、図12では、第1実施例(第1発明及び第2発明に対応)におけるセンタ10、ユーザ端末12の構成が各々説明されている。

【0078】図11のセンタ10は、秘密鍵ファイル装置100、制御回路102、データファイル装置104、秘密鍵生成起動回路106、グループ通信起動回路108、乱数発生回路110、暗号回路112、114、鍵選択回路116、多重化装置118、同報通信装置120で構成されている。

【0079】そのセンタ10の制御回路102から秘密鍵作成命令が送出されると、秘密鍵生成起動回路106が起動されてツリーが作成され、ノード識別番号がグループ通信起動回路108に格納される。

【0080】また乱数発生回路110も起動されてその乱数がマスタキーのデータとされ、各ユーザ端末12に関するこのマスタキーのデータとノード固有番号の定義内容が秘密鍵ファイル装置100に格納される。以上のようにして得られたノード識別番号、マスタキーデータは該当のユーザ端末12へ秘密鍵としてツリー構造に従い秘密配布される。

【0081】グループ送信の開始時には、グループ送信の開始命令とグループメンバーのユーザ端末12を特定するデータとが制御回路102からグループ通信起動回路108に与えられ、グループ通信起動回路108でグループ鍵の配送モードが選択される。

【0082】グループ鍵配送モードの動作がグループ通信起動回路108で開始されると、グループメンバーのユーザ端末12のみが自己より下位側のレイヤに存在するノードの固有番号（節点情報）が特定される。

【0083】このノード固有番号はグループ通信起動回路108から鍵選択回路116に送られて秘密鍵ファイル装置100の参照に使用され、その結果、該当のマスタキーデータ（秘密鍵）が秘密鍵ファイル装置100から取り出され、鍵選択回路116から暗号回路112に与えられる。

【0084】一方、グループ通信起動回路108により乱数発生回路110が起動されて乱数のセッションキーデータが生成され、そのセッションキーデータも暗号回路112に与えられる。

【0085】暗号回路112ではマスタキーデータによりセッションキーデータが暗号化され（暗号化セッション鍵）、また、暗号回路114ではグループ送信の対象となるデータファイル装置104のデータが、暗号化されたセッションキーデータより、暗号化される。

【0086】多重化装置118にはノード識別番号、暗号化されたセッションキーデータ、暗号化された同報送信データが与えられ、それらは多重化装置118で多重化されてから同報装置120からスター状のネットワーク14へ送出される。

【0087】図12のユーザ端末12は、信号受信・多重分離装置200、グループ通信検出回路20、鍵選択回路204、秘密鍵ファイル装置206、暗号回路208、暗号回路210、これらを制御する制御回路212、データファイル装置214、1/O装置216で構成されている。

【0088】なお、配布されたマスタキーデータは秘密鍵ファイル装置206に格納され、自端末12に割り付けられたノード固有番号はグループ通信検出回路202と鍵選択回路204に格納される。

【0089】上記のセンタ10からネットワーク14へ送出されたノード識別番号、セッションキーデータ、同報送信データは信号受信・多重化分離装置200で信号受信され、分離される。

【0090】これらのうち、ノード識別番号はグループ通信検出回路202で配布済みのノード識別番号と突き合わされ、その結果から、自端末12がグループ通信のメンバーか否かが調べられる。

【0091】グループメンバーであることが確認されると、グループ通信検出回路202によって鍵選択回路204が起動され、秘密鍵ファイル装置206から鍵選択回路204へ配布済みのマスタキーデータが取り出される。

【0092】そのマスタキーデータは暗号回路208に与えられ、暗号回路208では信号受信・多重化分離装置200から与えられたセッションキーデータが復号される（マスタキーでセッションキーのロックを解除する）。

【0093】さらに、セッションキーのデータは暗号回路208から暗号回路210に与えられ、暗号回路210では信号受信・多重化分離装置200から与えられた同報送信データがセッションキーデータを用いて復号される（セッションキーで受信データのロックを解除する）。

【0094】暗号回路210によって復号された同報送信データは、データファイル装置214に格納され、あるいは、1/O装置を介して外部へ出力され、したがって、ノード識別番号で指定されたユーザ端末12のみが、この同報送信データを受信出力できる。

【0095】以上の本実施例によれば、図13からも理解されるように、ユーザ端末12が保管すべき秘密鍵の数をわずかなものに抑制しながら、鍵配送回数の増加を回避することが可能となる。

【0096】図14、図15では、第2実施例（第3発明及び第4発明／第5発明、第6発明及び第7発明に対応）におけるセンタ10、ユーザ端末12の構成が説明されている。

【0097】図14においてセンタ10は、秘密鍵ファイル装置100（素数 $p$ 、 $q$ 、最小公倍数 $L$ が秘密情報として格納されている）、公開鍵ファイル装置101（乗算結果 $n$ が公開情報として格納されている）、制御回路102、データファイル装置104、秘密鍵生成起動回路106、グループ通信起動回路108、乱数発生回路110、暗号回路112、114、鍵生成回路117、多重化装置118、同報通信装置120で構成されている。

【0098】制御回路102から秘密鍵生成起動回路106に秘密鍵の作成命令が送出されると、秘密鍵生成起動回路106で図4または図7のツリーが生成される。このツリーはグループ通信起動回路108に格納され



る。

【0099】また、乱数発生回路110が起動されてノード固有番号と乱数（マスタキーデータ）とが各ノードに割り付けられ（マスタキーデータは仮割り付けされる）、それらがツリー公開鍵のデータとして鍵生成回路117に与えられる。

【0100】鍵生成回路117では公開鍵のマスタデータが所定の条件を満たしているか否かが検査され（最小公倍数 $\lambda$ と互いに素となるか否かの検査）、満たしていない場合には、乱数再発生指示が乱数発生回路110に与えられる。

【0101】その後、全てのユーザ端末12について公開鍵のマスタデータが得られると、秘密鍵（ $1/K_{ij}$ のみ、または、 $1/K_{ij}$ 及び $1/KK_{ij}$ ）のデータが生成される。なお、全ユーザ端末12の秘密鍵と公開鍵は秘密鍵ファイル装置101、公開鍵ファイル100に各々格納される。

【0102】さらに各ユーザ端末12のパスワード入力開始され、パスワードの入力毎に鍵生成データ（キー生成データ $Z_s$ ：図5、図9参照）が作成される（パスワードの入力毎にそのパスワードが最小公倍数 $\lambda$ と互いに素となるか否かが検査される。また、該当の秘密鍵のデータが存在しているか否かもチェックされる。秘密鍵のデータが存在していた場合で、パスワードが最小公倍数 $\lambda$ と互いに素となるときには、そのパスワードを用いてキー生成データが作成される。該当の秘密鍵データが存在していなかった場合、または、パスワードが最小公倍数 $\lambda$ と互いに素とならない場合、別のパスワードが再び入力される）。このようにして作成されたキー生成データは該当のユーザ端末12へ公開鍵のデータ（ノード固有番号を含む）とともに配布される。

【0103】全てのユーザ端末12にキー生成データが配布された後に、グループ送信が行なわれる。その際には、制御回路100からグループ送信の起動命令とグループ情報とがグループ通信起動回路108に与えられる。

【0104】グループ通信起動回路108では、同報先となるユーザ端末12のみがツリーの下位側に含まれるノードの固有番号を全て求める処理が行なわれ、これらのノード固有番号は鍵生成回路117に与えられる。

【0105】鍵生成回路117においては、公開鍵ファイル装置101から公開鍵のデータを取り出し、各ノードに対応する鍵暗号化鍵のデータ（キー暗号化キーデータ $KGK_j$ ：図10参照）を生成する処理が行なわれ、鍵生成回路117が生成したキー暗号化キーのデータは暗号回路112に与えられる。

【0106】このときにグループ通信起動回路108で乱数発生回路110も起動され、セッション鍵のデータ（セッションキーデータ）が生成される。そのセッションキーデータは暗号回路112に与えられ、鍵生成回路

117で生成されたキー暗号化キーデータにより暗号化される（暗号化セッションキー）。

【0107】また、乱数のセッションキーデータは暗号回路114にも送付され、データファイル装置104から読み出されたグループ送信用のデータがこのセッションキーデータで暗号化される。

【0108】以上のノード固有番号、暗号化されたセッションキーデータ、暗号化された同報送信データは多重化装置118で多重化されてから、同報装置120よりスター状のネットワーク14へ送出される。

【0109】図14において各ユーザ端末12は、信号受信・多重分離装置200、グループ通信検出回路202、鍵生成回路204、公開鍵ファイル装置207、暗号回路208、暗号回路210、これらを制御する制御回路212、データファイル装置214、I/O装置216で構成されている。

【0110】なお、キー生成データとノード固有番号はグループ通信検出回路202、鍵生成回路204に格納される。また、公開鍵のデータは公開鍵ファイル207に格納される。そして、キー生成データはユーザの所持する磁気カードあるいはICカードに書き込まれる。さらに、パスワードは各ユーザによって管理される。

【0111】センタ10がネットワーク14へ送出したノード固有番号、セッションキーデータ、グループ送信データは信号受信・多重化分離装置200で信号受信され、分離される。

【0112】これらのうち、ノード固有番号（接点情報）はグループ通信検出回路202に与えられ、配布されたノード固有番号との突合せで自端末12がグループ通信のメンバーか否かが判定される。

【0113】グループメンバーの場合には、グループ通信検出回路202により鍵生成回路204が起動され、鍵生成回路204では公開鍵ファイル装置207の公開鍵データ、配布されたキー生成データ、ユーザから入力されたパスワードを用いてキー暗号化キーデータ（鍵暗号化鍵のデータ）が作成される。

【0114】作成されたキー暗号化キーデータは暗号回路208に与えられる。この暗号回路208には信号受信・多重分離装置200からセッションキーデータ（暗号化されている）が与えられ、そのセッションキーデータはキー暗号化キーデータを用いて復号される。

【0115】そして、復号されたセッションキーデータは、暗号回路210に与えられる。暗号回路210には信号受信・多重分離装置200からグループ通信データ（暗号化されている）が与えられ、このグループ送信データは暗号回路208から与えられたセッションキーデータを用いて復号される。

【0116】このようにして暗号回路210で復号されたグループ送信データはデータファイル装置214に格納され、あるいは、I/O装置216を介して外部へ出



力される。

【0117】図16(A)では第3発明、第4発明が適用されたときに鍵生成回路204で行なわれる処理の手順がフローチャートを用いて説明されており、また、同図(B)では第5発明、第6発明、第7発明が適用されたときの処理手順が説明されている。

【0118】図16(A)、(B)において、センタ10から受信したノード固有番号、配布されたキー生成データ、ユーザ入力のパスワード、公開ファイル装置207のノード固有番号及びマスタキーデータが順に入力される(ステップ1600、1602、1604、1606)。

【0119】そして第3発明、第4発明が適用されたときには図17の処理手順でキー暗号化キーデータが作成される(ステップ1700)。また、第5発明、第6発明、第7発明が適用されたときには最下位のレイヤ内でユーザ端末12をグループ化しているか否かが判断される(ステップ1608)、その判断結果に応じ、図18あるいは図19の処理手順で、キー暗号化キーデータが作成される(ステップ1800、1900)。

【0120】図17においては、キー作成データにマスタキーデータを巾乗する処理(ステップ1702)と、キー作成データにパスワードを巾乗する処理(ステップ1704)とが行なわれる。

【0121】図18の処理は最下位のレイヤ内でユーザ端末12をグループ化しているときに行なわれ、最初にキー作成データへグループキーデータが巾乗され(ステップ1802)、次に、キー作成データへパスワードが巾乗される(ステップ1704)。

【0122】図19の処理は最下位のレイヤ内でユーザ端末12をグループ化していないときに行なわれ、最初に、キー作成データへグループキーデータが巾乗され(ステップ1902)、次に、キー作成データへマスタキーデータが巾乗され(ステップ1904)、最後に、キー作成データへパスワードが巾乗される(ステップ1906)。

【0123】以上の本実施例によれば、図13からも理解されるように、第1実施例に比してユーザ端末12側における秘密鍵の保管数を削減(第3発明、第4発明の適用時)し、あるいは、公開鍵保管数のわずかな増加と引き換えに鍵配送数を大幅に削減(第5発明、第6発明、第7発明の適用時)することが可能となる。

【0124】なお、乱数発生回路110に代えて素数発生回路を設け、鍵生成回路117の処理を簡便化することも可能であり、また、各レイヤの分岐数を3以上として鍵配送数を削減することも好適である。

【0125】

【発明の効果】以上説明したように本発明によれば、センタから各ユーザ端末に至るツリー構造の採用で、鍵配送の所要時間を短縮することが可能となり、また、各ユ

ーザ端末で保管される秘密鍵の数を削減することも可能となる。

【図面の簡単な説明】

【図1】第1発明及び第2発明の原理説明図である。

【図2】第3発明及び第4発明の原理説明図である。

【図3】第5発明、第6発明及び第7発明の原理説明図である。

【図4】バイナリツリーの説明図である。

【図5】キー生成データを作成する処理の内容説明図である。

【図6】第3発明及び第4発明の作用説明図である。

【図7】第5発明、第6発明及び第7発明におけるツリー及びキー生成データの説明図である。

【図8】第5発明、第6発明及び第7発明における最下位レイヤのユーザグループ化作用説明図である。

【図9】第5発明、第6発明及び第7発明におけるキー生成データの作成作用説明図である。

【図10】第5発明、第6発明及び第7発明におけるユーザ端末のキー暗号化キー作成作用説明図である。

【図11】第1実施例におけるセンタの構成説明図である。

【図12】第1実施例におけるユーザ端末の構成説明図である。

【図13】発明の効果説明図である。

【図14】第2実施例におけるセンタの構成説明図である。

【図15】第2実施例におけるユーザ端末の構成説明図である。

【図16】第2実施例におけるユーザ端末で行なわれる処理の手順を説明するフローチャートである。

【図17】第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャートである。

【図18】第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャートである。

【図19】第2実施例におけるユーザ端末の鍵生成手順を説明するフローチャートである。

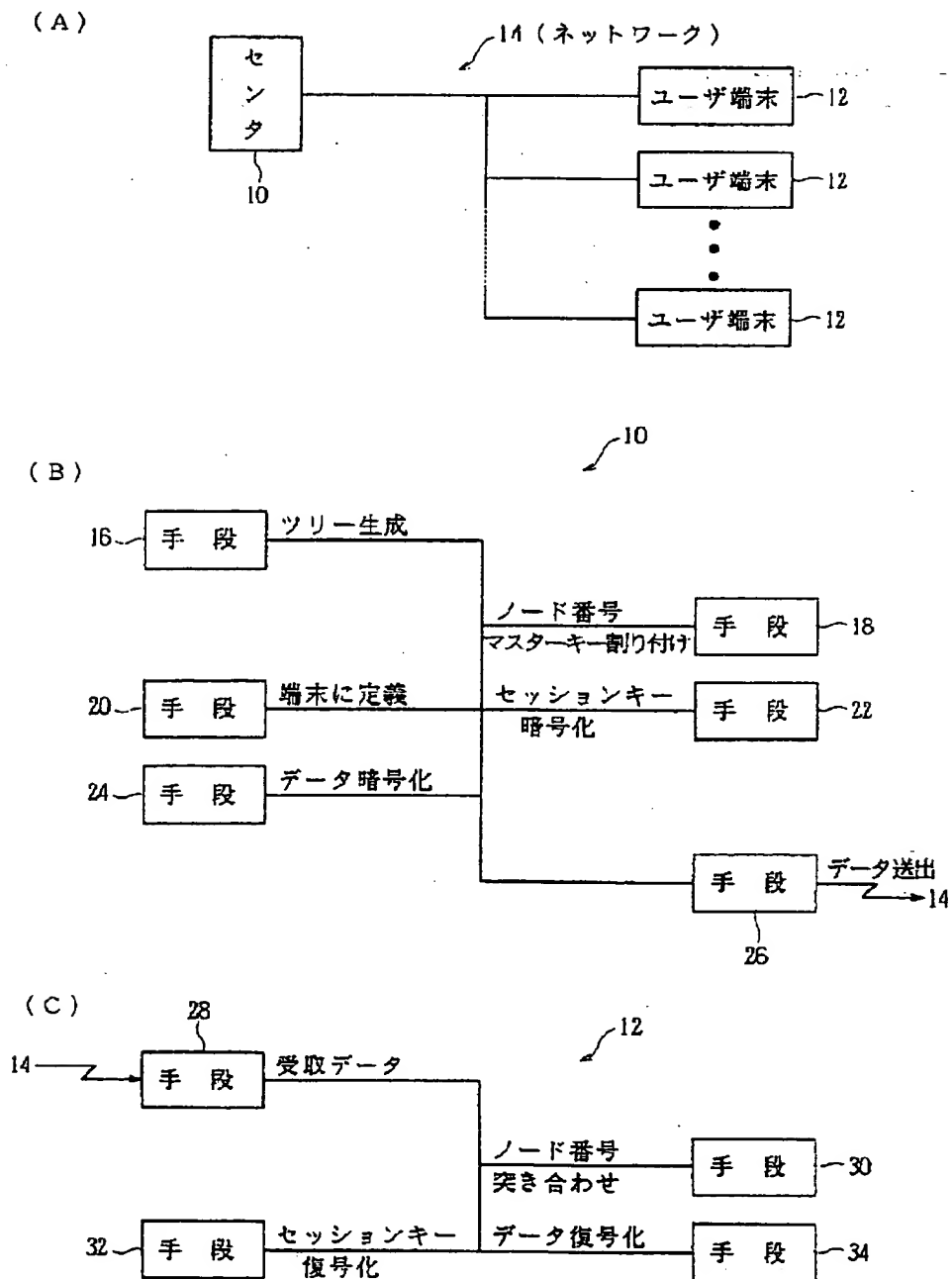
【符号の説明】

10	センタ
12	ユーザ端末
14	ネットワーク
100	秘密鍵ファイル装置
101	公開鍵ファイル装置
102	制御回路
104	データファイル装置
106	秘密鍵生成起動回路
108	グループ通信起動回路
110	乱数発生回路
112、114	暗号回路
116	鍵選択回路
117	鍵生成回路

- |     |             |          |           |
|-----|-------------|----------|-----------|
| 118 | 多重化装置       | 207      | 公開鍵ファイル装置 |
| 120 | 同報装置        | 208, 210 | 暗号回路      |
| 200 | 信号受信・多重分離装置 | 212      | 制御回路      |
| 202 | グループ通信検出回路  | 214      | データファイル装置 |
| 204 | 鍵選択回路       | 216      | 1/O装置     |
| 206 | 秘密鍵ファイル装置   |          |           |

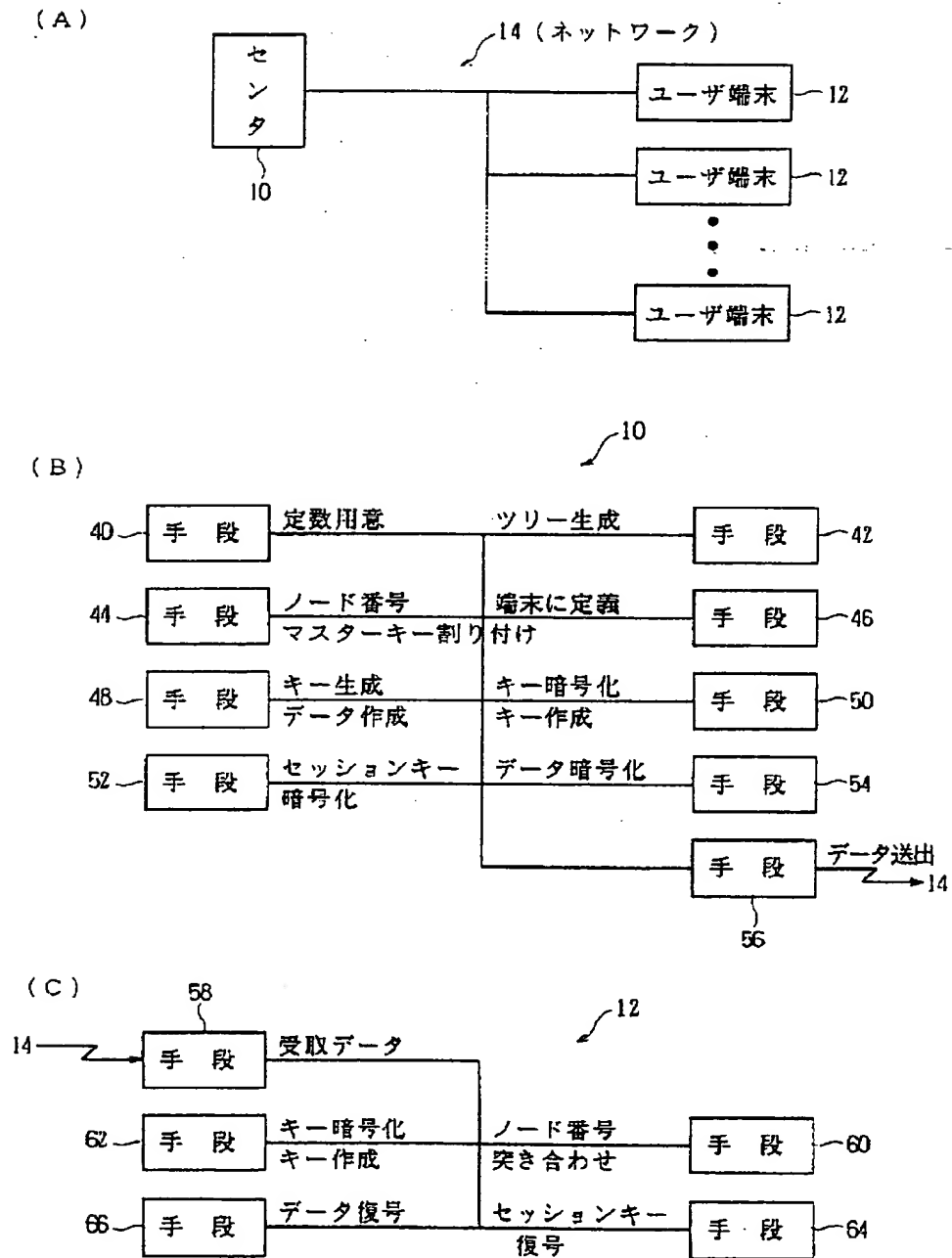
【図1】

## 第1発明及び第2発明の原理説明図



【図2】

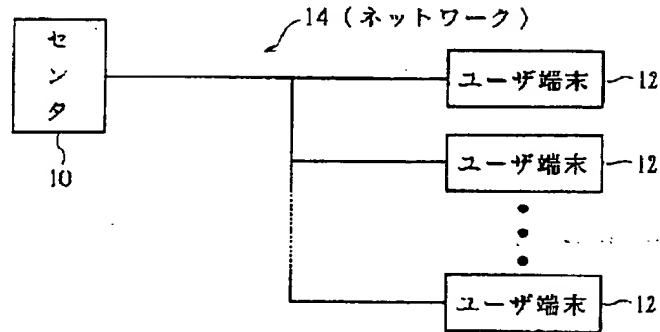
## 第3発明及び第4発明の原理説明図



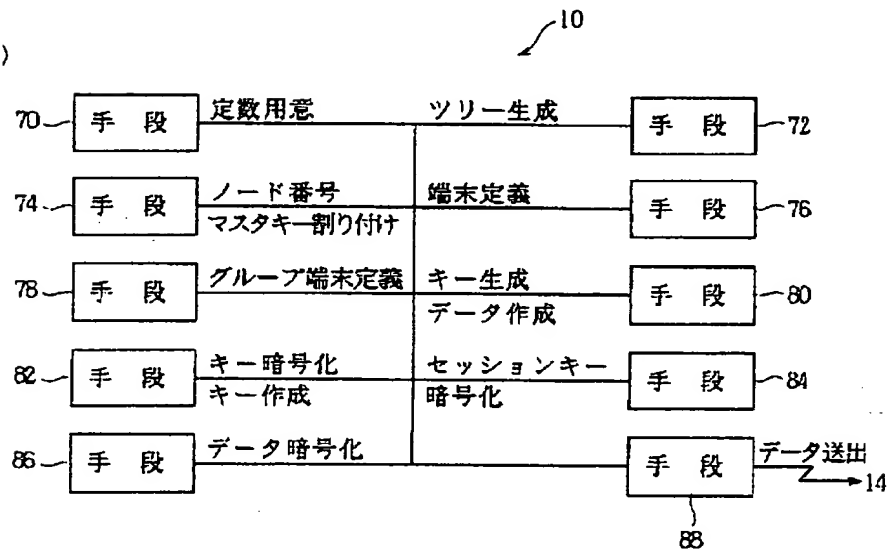
【図3】

第5発明、第6発明及び第7発明の原理説明図

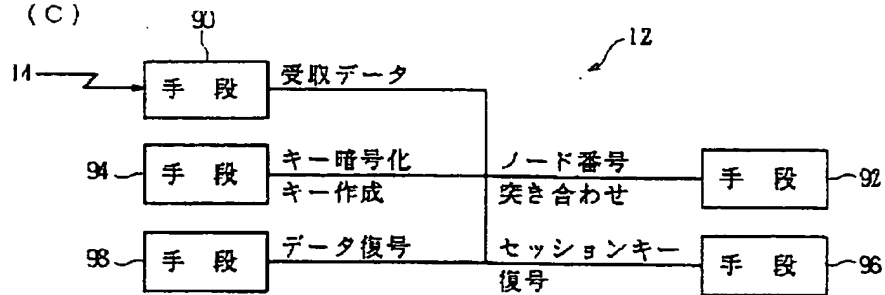
(A)



(B)

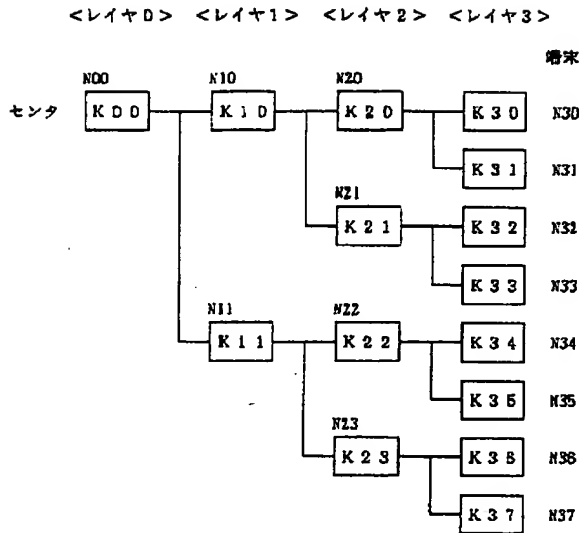


(C)



【図4】

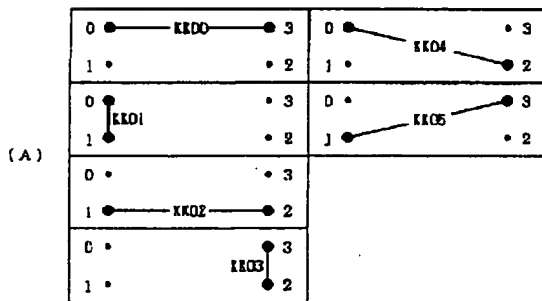
バイナリツリーの説明図



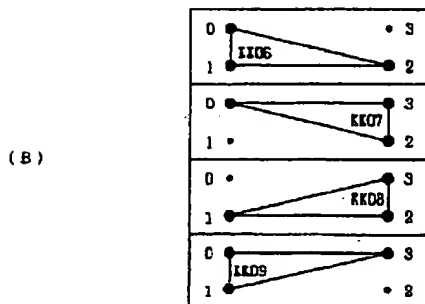
【図8】

第5発明、第6発明及び第7発明における再下位レイヤのユーザーグループ化作用説明図

&lt;2ユーザーのグループ化&gt;



&lt;3ユーザーのグループ化&gt;



【図5】

キー生成データを作成する処理の内容説明図

$$Zs = C^{**} (1 / (PWs * Ks)) \bmod n$$

C : センタのID情報, 有効期間等  
 Ks : ユーザsに割当られた公開鍵の集合の積  
 $Ks = \prod Kij$   
 $\{Kij\} \in Us$  内容説明図

【図9】

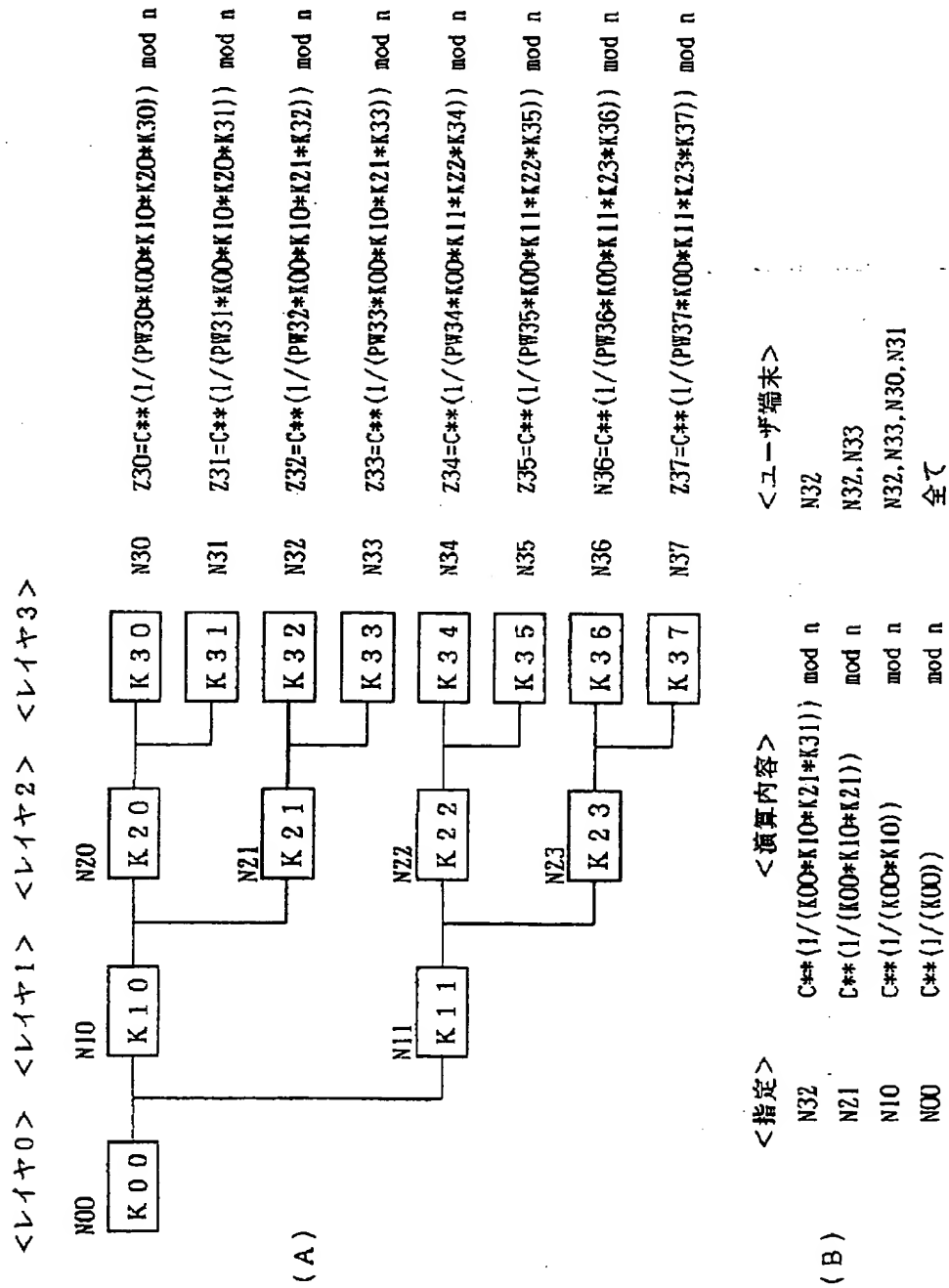
第5発明、第6発明及び第7発明におけるキー生成データの作成作用説明図

$$Zs = C^{**} (1 / (PWs * Ks * KKs)) \bmod n$$

C : センタのID情報, 有効期間等  
 Ks : ユーザsに割当られたツリー公開鍵の集合の積  
 $Ks = \prod Kij$   
 $\{Kij\} \in Us$   
 KKs : ユーザsに割当られたグループ公開鍵の集合の積  
 $KKs = \prod KKij$   
 $\{KKij\} \in Us$

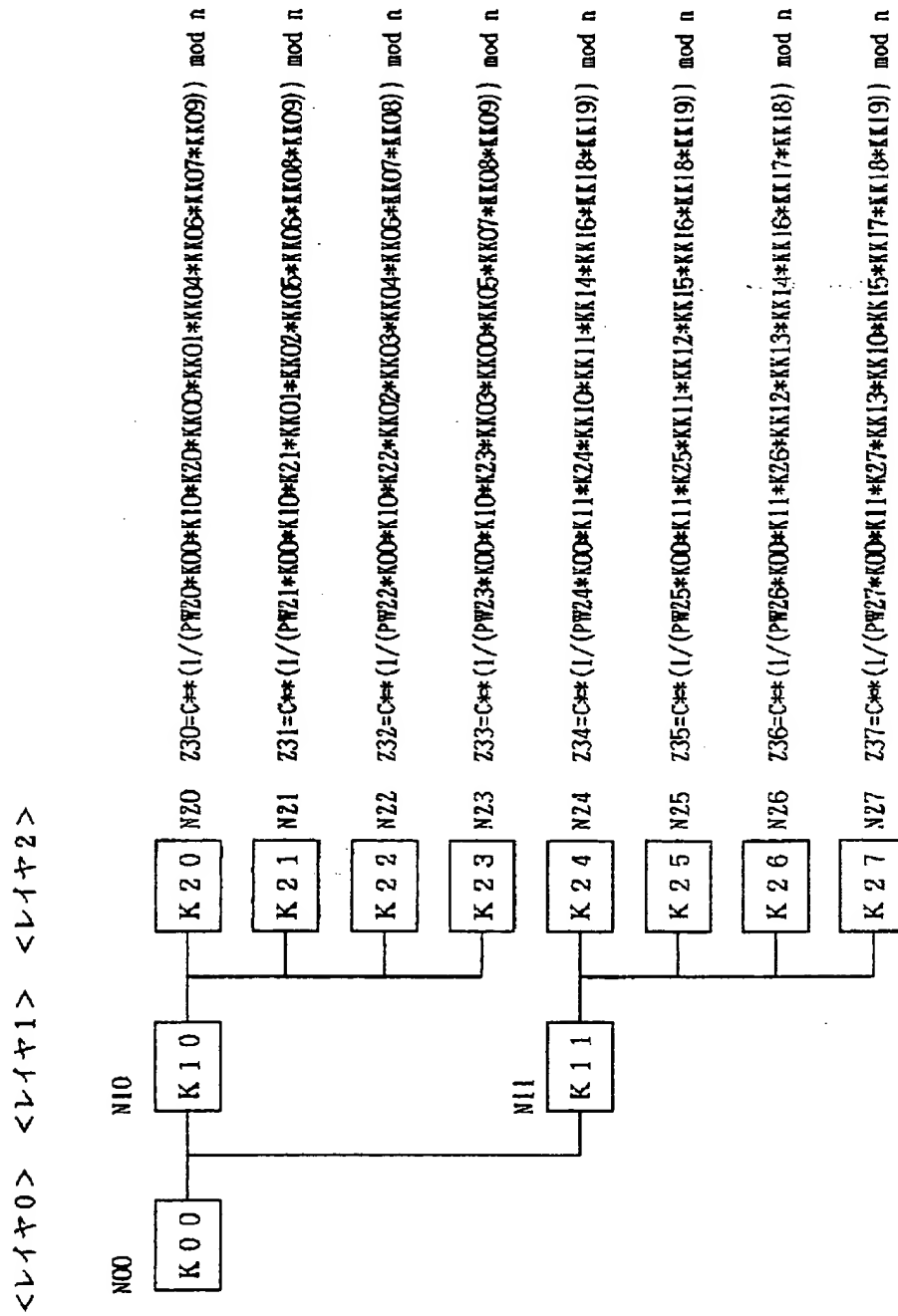
【図 6】

## 第 3 発明及び第 4 発明の作用説明図



【図7】

第5発明、第6発明及び第7発明におけるツリー及びキー生成データの説明図



【図 10】

第 5 発明、第 6 発明及び第 7 発明におけるユーザ端末のキー暗号化キー作成作用説明図

(A)

$$\begin{aligned}
 KGK_j &= Z_j^{**} \left( PW_j * K_{k-1,j} * K_{k-2,j} * \dots * K_{r,j} * \prod_{m=0}^{Ng-1} KK_{j,m} \right) \bmod n \\
 &= C^{**} (1 / (K_{0,j} * \dots * K_{k,j})) \bmod n
 \end{aligned}$$

(B)

$$\begin{aligned}
 KGK_j &= Z_j^{**} \left( PW_j * \left( \prod_{m=0}^{Ng-1} KK_{j,m} \right) / KK_{j,c} * K_{r,j} \right) \bmod n \\
 &= C^{**} (1 / (K_{0,j} * \dots * K_{r-1,j} * K_{k,j,q})) \bmod n
 \end{aligned}$$

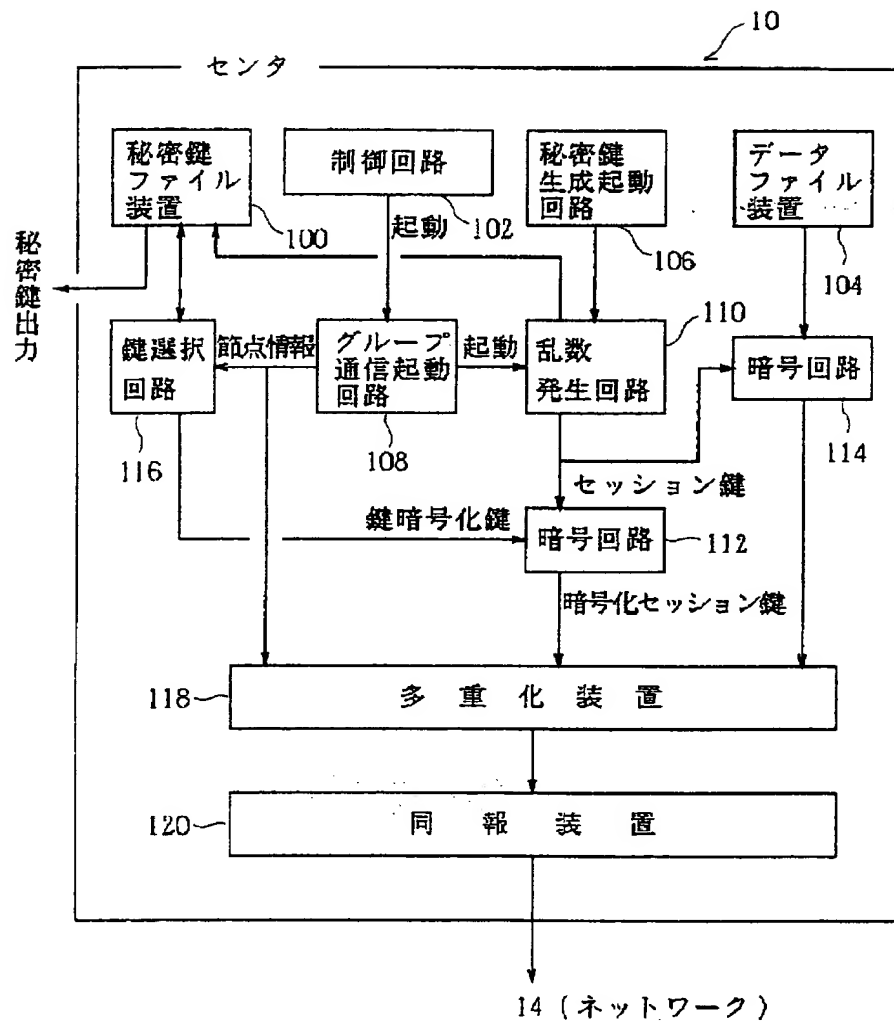
(C)

<指定>	<演算内容>	<ユーザ端末>
N00	$C^{**} (1 / (K_{00})) \bmod n$	全て
N10	$C^{**} (1 / (K_{00} * K_{10})) \bmod n$	N20, N21, N22, N23
N22	$C^{**} (1 / (K_{00} * K_{10} * K_{22})) \bmod n$	N22
31-サ	$C^{**} (1 / (K_{00} * K_{10} * K_{08})) \bmod n$	N20, N21, N22
21-サ	$C^{**} (1 / (K_{00} * K_{10} * K_{04})) \bmod n$	N20, N22



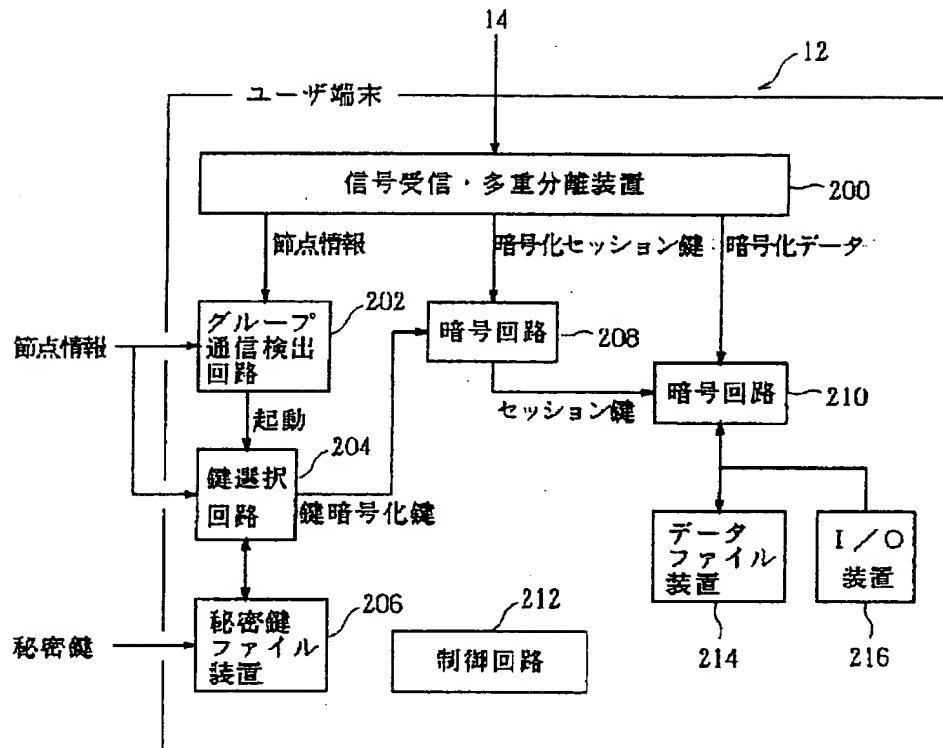
【図11】

## 第1実施例におけるセンタの構成説明図



【図 12】

第 1 実施例におけるユーザ端末の構成説明図



【図13】

発明の効果説明図

<ユーザ端末の総数：128>

方 式	センタ側		ユーザ側		鍵配送数			
	秘密鍵数	公開鍵数	秘密鍵数	公開鍵数	Ng=32	Ng=64	Ng=96	Ng=127
通信毎全配布	128		128		32	64	96	127
全鍵保管方式	2**128-1		2**127-1		0	0	0	0
第1及び第2発明	128		128		32*	64*	64*	7*
第3及び第4発明	254	254	1	8	32*	64*	64*	7*
第5,第6(1ツリー及びグループ)第7発明	158 3952	158 3952	1	5 247	16*	16*	16*	5*

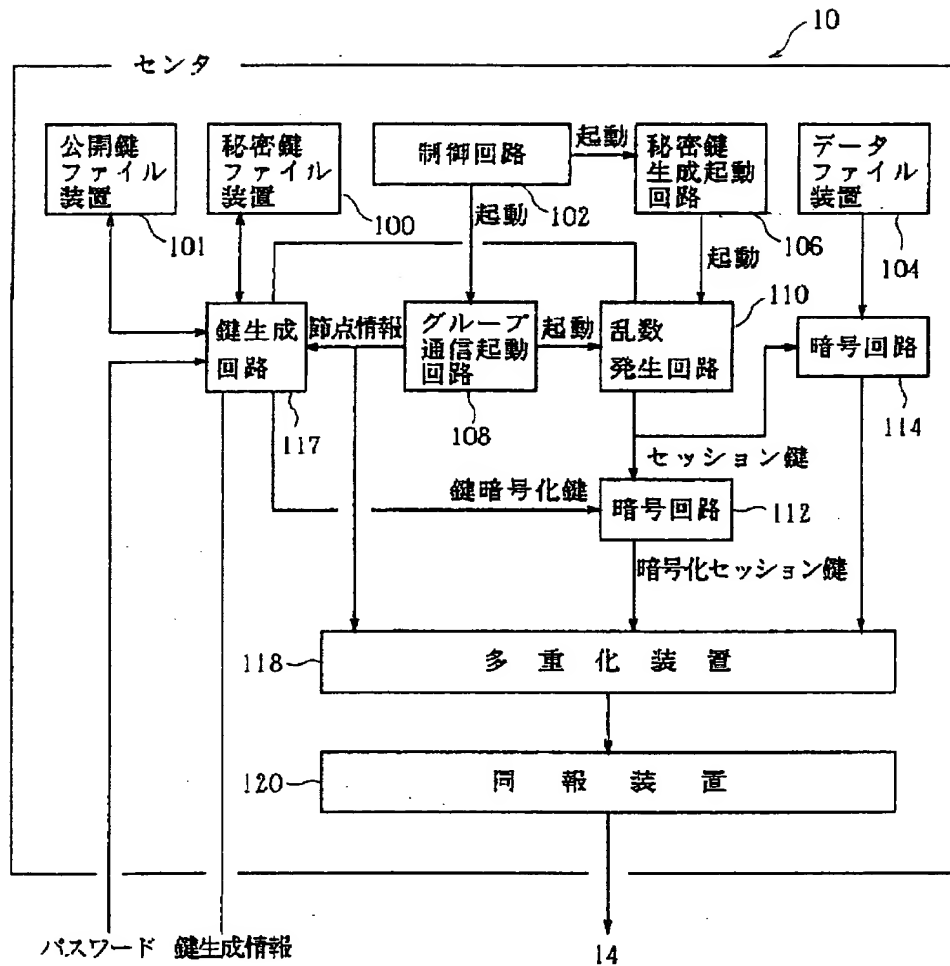
Ng：グループ内ユーザ数

\*：最悪値

1：最終点での分岐を8とする

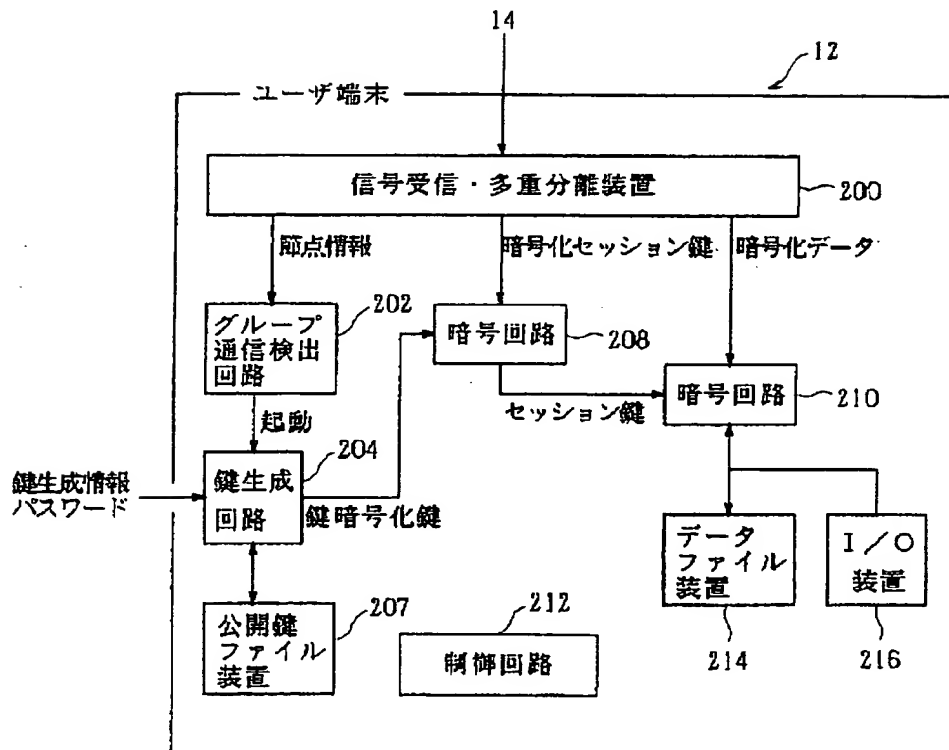
【図14】

第2実施例におけるセンタの構成説明図



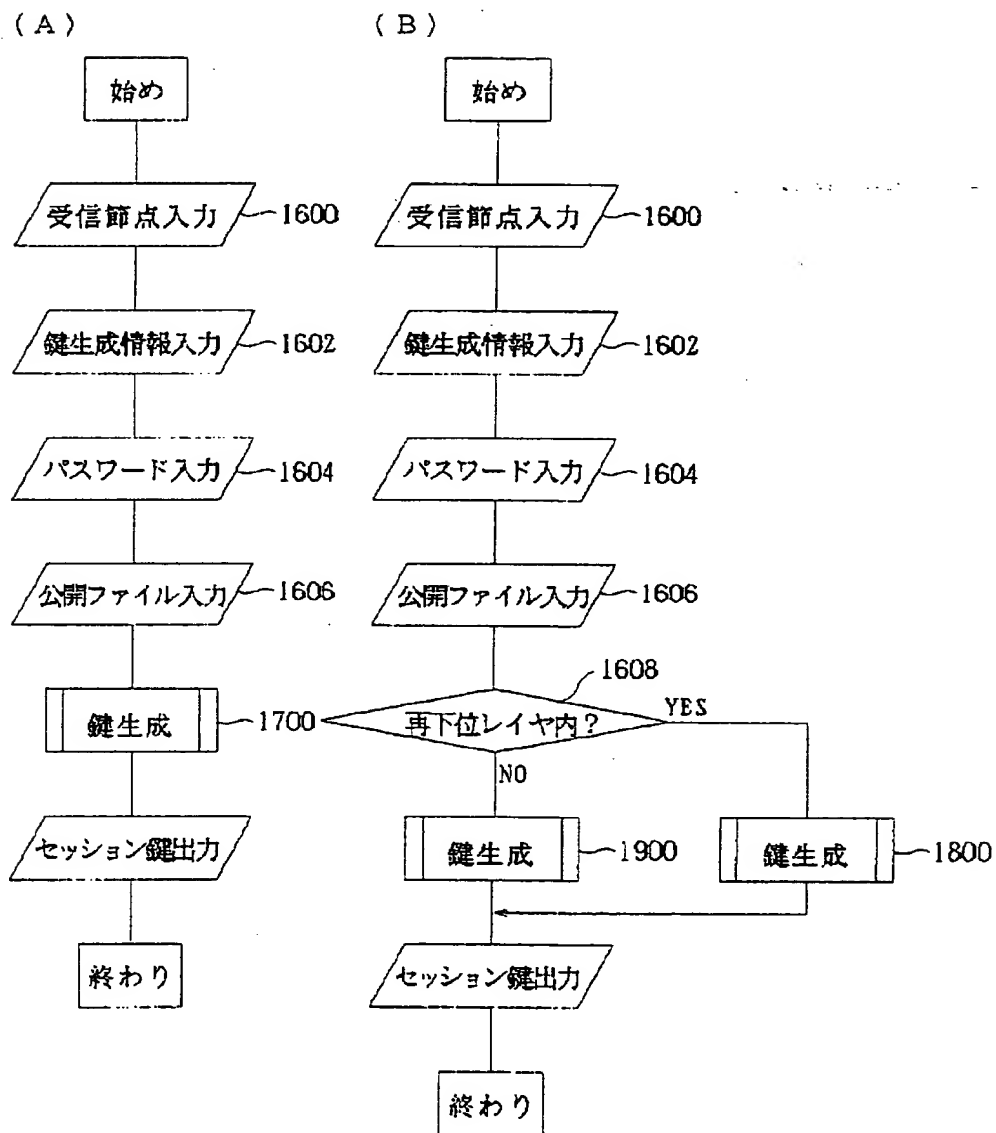
【図15】

第2実施例におけるユーザ端末の構成説明図



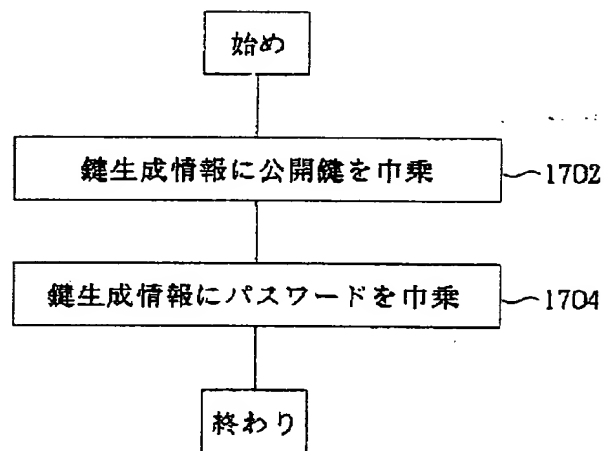
【図 16】

第 2 実施例におけるユーザ端末の行われる処理の手順を説明するフローチャート



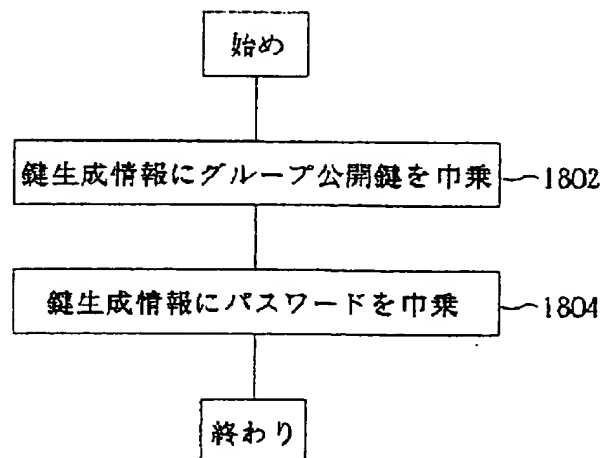
【図 17】

第 2 実施例におけるユーザ端末の鍵生成手順を説明する  
フローチャート



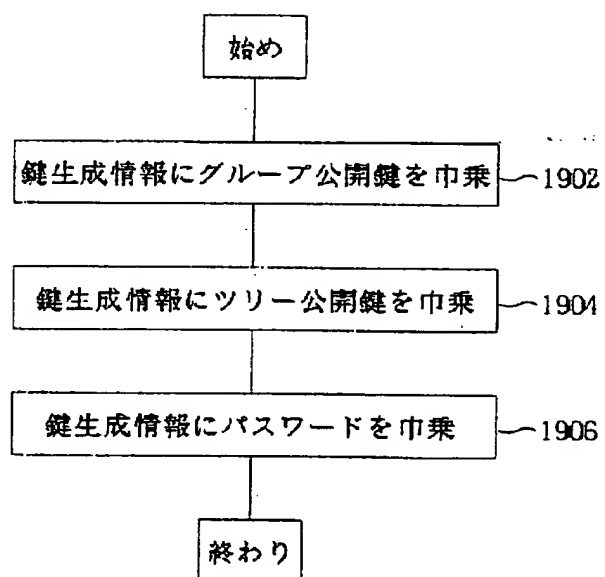
【図 18】

第 2 実施例におけるユーザ端末の鍵生成手順を説明する  
フローチャート



【図 19】

第 2 実施例におけるユーザ端末の鍵生成手順を説明する  
フローチャート



フロントページの続き

(51) Int. Cl. 5

H 0 4 L 9/06

9/14

識別記号

庁内整理番号

F I

技術表示箇所